The Structure of Linear Codes of Constant Weight

Jay A. Wood

Department of Mathematics and Statistics, Western Michigan University, 1903 W. Michigan Ave., Kalamazoo, MI 49008–5248

Abstract

In this paper we determine completely the structure of linear codes over $\mathbb{Z}/N\mathbb{Z}$ of constant weight. Namely, we determine exactly which modules underlie linear codes of constant weight, and we describe the coordinate functionals involved. The weight functions considered are: Hamming weight, Lee weight, and Euclidean weight. We present a general uniqueness theorem for virtual linear codes of constant weight. Existence is settled on a case by case basis.

Key words: Constant weight codes, Lee weight, Euclidean weight, extension theorem, virtual codes

1 Introduction

This paper classifies the structure of linear codes of constant weight over $\mathbb{Z}/(N) = \mathbb{Z}/N\mathbb{Z}$. A linear code having constant weight means that every nonzero codeword has the same weight. Hamming, Lee, and Euclidean weights are all examined.

The classification specifies which modules over $\mathbb{Z}/(N)$ underlie linear codes of constant weight, and it specifies what the coordinate functionals need to be (up to an appropriate notion of equivalence).

There are a few surprises. While constant Hamming weight codes exist in all dimensions over finite fields, they almost never exist over the $\mathbb{Z}/(N)$'s that are not fields. Constant Lee or Euclidean weight codes exist for any module

Email address: `jay.wood@wmich.edu`, `http://unix.cc.wmich.edu/jwood` (Jay A. Wood).

Preprint submitted to Elsevier Preprint *22 November 2000*

over $\mathbb{Z}/(2^\beta)$, but are comparatively rare over the $\mathbb{Z}/(N)$'s that have odd prime factors in N.

The classification has two aspects: uniqueness and existence. By utilizing what we call virtual linear codes, we find that, for a given R-module M, there is a one-dimensional rational vector space of constant weight virtual linear codes supported by M. Uniqueness results then follow immediately.

By knowing that there is a one-dimensional solution space, existence questions reduce to "guess and check." That is, we guess (guided by calculations) the format of a solution, and then we verify that it indeed has constant weight. Due to space limitations, we will simply state the form of the solutions.

2 Linear Codes over Finite Rings

In this paper, any ring denoted by R will be assumed to be a finite commutative ring with 1. The ideal generated by $r \in R$ will be denoted by (r). Any R-module M will be assumed to be finitely generated and unital, i.e., $1 \in R$ acts as the identity. The linear dual of M is denoted $M^\sharp := \mathrm{Hom}_R(M, R)$. The elements of $M^\sharp$ are the *linear functionals* on M. Integer residue rings are denoted $\mathbb{Z}/(N) := \mathbb{Z}/N\mathbb{Z}$. The natural numbers $\mathbb{N}$ will contain 0. The number of elements in a finite set S is $|S|$.

Let $R = \mathbb{Z}/(N)$, with prime factorization

$$N = p_1^{\beta_1} \dots p_l^{\beta_l}. \tag{2.1}$$

Every module M over R has a direct sum decomposition

$$M \cong \bigoplus_{i=1}^{l} \bigoplus_{j=1}^{\beta_i} \left(\mathbb{Z}/(p_i^j)\right)^{k_{i,j}}, \tag{2.2}$$

for appropriate non-negative integers $k_{i,j}$. Observe that

$$|M| = \prod_{i=1}^{l} p_i^{\sum_{j=1}^{\beta_i} j k_{i,j}}.$$

To avoid the situation where M is actually a pullback of a module defined over a quotient ring of R, we assume that, for all i,

$$k_{i,\beta_i} \geq 1. \tag{2.3}$$

There will be occasions where the prime number 2 will occur explicitly in (2.1). In that case $2 = p_0$ with exponent β_0 and integers $k_{0,j}$ in (2.2).

Linear codes will be described from the linear functional point of view of [1], although phrased in a slightly different way. A *linear code* C over R is a pair (M, η), where M is an R-module, the module *underlying* the code, and $\eta : M^\sharp \to \mathbb{N}$ is a *multiplicity function*. The *length* n of the linear code C is $n = \sum_{\lambda \in M^\sharp} \eta(\lambda)$. A linear code is *nondegenerate* if the multiplicity of the zero functional vanishes, i.e., if $\eta(0) = 0$.

A linear code (M, η) determines a linear homomorphism $\phi_\eta : M \to R^n$, $x \mapsto (\lambda(x))_{\lambda \in M^\sharp}$, where the entry $\lambda(x)$ appears $\eta(\lambda)$ times. The image of ϕ_η is a submodule of R^n, and this submodule is a linear code in the classical sense. In defining ϕ_η one must choose an order in which to write down the terms $\lambda(x)$.

We shall usually assume that (M, η) satisfies the *coding axiom*, which states that ϕ_η is injective. By passing to a quotient, $M/\ker \phi_\eta$, the coding axiom holds automatically.

One way to view the definition above is to recall that a linear code is determined by its generator matrix G. The columns of G are given by linear functionals. Up to permutations of coordinate positions (the choice of order in writing down the terms in ϕ_η), the code is determined by the multiplicities of the various columns of G. It is exactly this information which is encoded by the multiplicity function η.

A *virtual linear code* over a ring R is a pair (M, η), where M is an R-module and $\eta : M^\sharp \to \mathbb{Q}$ is a multiplicity function. Linear codes where η takes values in $\mathbb{N}$ will be called *classical* linear codes.

3 Weight Functions and the Extension Property

In order to define the weight of codewords, we first define a *weight function* w on the ring R by assigning real number weights a_r to every $r \in R$. We assume that $a_0 = 0$ and that $a_r > 0$ for $r \neq 0$. This choice of weight function on R allows us to define a *weight function* $w_\eta : M \to \mathbb{R}$ on any linear code $C = (M, \eta)$, classical or virtual:

$$w_\eta(x) = \sum_{\lambda \in M^\sharp} \eta(\lambda)\, a_{\lambda(x)}, \quad x \in M. \tag{3.1}$$

For example, Hamming weight uses $a_r = 1$, for all $r \neq 0$. We say that a linear code C has *constant weight* $L > 0$ if $w_\eta(x) = L$ for all nonzero $x \in M$. Since the zero element $0 \in M$ always has $w_\eta(0) = 0$, we hope the reader will tolerate this slightly misleading terminology.

To capture some of the symmetry of a weight function w, define the *symmetry group* of w to be

$$\mathrm{Sym}(w) := \{u \in \mathcal{U}(R) : a_{ur} = a_r, \text{ all } r \in R\},$$

where $\mathcal{U}(R)$ is the group of units of R. The group $\mathrm{Sym}(w)$ acts on both M and $M^\sharp$ by scalar multiplication, thereby decomposing M and $M^\sharp$ into $\mathrm{Sym}(w)$-orbits. Denote the $\mathrm{Sym}(w)$-orbits of $x \in M$ and $\lambda \in M^\sharp$ by $\mathrm{orb}(x)$ and $\mathrm{orb}(\lambda)$, respectively.

Consider a linear code (M, η) over R. For any $\lambda \in M^\sharp$, define a symmetrized version η_S of η by

$$\eta_S(\lambda) := \sum_{\mu \in \mathrm{orb}(\lambda)} \eta(\mu). \tag{3.2}$$

Then $\eta_S(\lambda)$ is the total multiplicity of linear functionals that belong to $\mathrm{orb}(\lambda)$. Clearly, $\eta_S(\lambda) = \eta_S(\mu)$ if $\mu \in \mathrm{orb}(\lambda)$. Note that (3.1) can be rewritten as

$$w_\eta(x) = \sum_{\lambda:\ \mathrm{rep}} \eta_S(\lambda)\, a_{\lambda(x)}, \quad x \in M, \tag{3.3}$$

where the summation is over one representative λ of each $\mathrm{Sym}(w)$-orbit.

Two linear codes $C' = (M, \eta')$, $C = (M, \eta)$, are *scale equivalent* if $\eta'_S = \eta_S$. Let $\mathcal{O}$, $\mathcal{O}^\sharp$ denote the sets of nonzero $\mathrm{Sym}(w)$-orbits on M, $M^\sharp$, respectively. Denote the set of all functions $\mathcal{O}^\sharp \to \mathbb{N}$ (resp., $\mathbb{Q}$) by $\mathbb{N}[\mathcal{O}^\sharp]$ (resp., $\mathbb{Q}[\mathcal{O}^\sharp]$).

Theorem 3.1 *Fix an R-module M. There is a bijection between the set of all nondegenerate classical (resp., virtual) linear codes (M, η), up to scale equivalence, and the function space $\mathbb{N}[\mathcal{O}^\sharp]$ (resp., $\mathbb{Q}[\mathcal{O}^\sharp]$).*

Two linear codes $C' = (M', \eta')$, $C = (M, \eta)$, are *equivalent* if there exists an isomorphism $f : M' \to M$ such that $(M, \eta' \circ f^\sharp)$ and (M, η) are scale equivalent. If C' and C are equivalent, a re-indexing argument shows that $w_{\eta'}(x) = w_\eta(f(x))$ for all $x \in M'$. That is, f induces a weight-preserving isomorphism between the codes. The converse of this statement is discussed next.

Definition 3.2 *A weight function w over a ring R has the* extension property *(EP) if:*

For any two linear codes $C' = (M', \eta')$, $C = (M, \eta)$ over R with an isomorphism $f : M' \to M$ satisfying $w_{\eta'}(x) = w_\eta(f(x))$ for all $x \in M'$, it follows that $(M, \eta' \circ f^\sharp)$ and (M, η) are scale equivalent. (Thus C', C are equivalent via f.)

If EP is satisfied, it follows that every weight preserving automorphism of R^n is a $\mathrm{Sym}(w)$-monomial transformation.

Theorem 3.3 *Suppose R, w satisfy EP and that M is a fixed R-module. Define a mapping $W : \mathbb{N}[\mathcal{O}^\sharp] \to \mathbb{R}[\mathcal{O}]$, $g \mapsto w_g$, where*

$$w_g(\mathrm{orb}(x)) = \sum_{\lambda:\ \mathrm{rep}} g(\mathrm{orb}(\lambda))\, a_{\lambda(x)},$$

and the summation is over one representative λ of each $\mathrm{Sym}(w)$-orbit. Then W is injective.

Example 3.4 *Hamming weight. Over any ring R, set $a_r = 1$ for $r \neq 0$; $a_0 = 0$. The symmetry group $\mathrm{Sym}(w) = \mathcal{U}(R)$, the full group of units of R. EP holds over finite fields ([4]). EP holds over any finite Frobenius ring ([5]).*

Example 3.5 *Lee weight on $R = \mathbb{Z}/(N)$. Choose representatives in the range $-N/2 < r \leq N/2$, and set $a_r = |r|$. It follows that $\mathrm{Sym}(w) = \{\pm 1\}$. EP has been numerically verified for $N \leq 256$ (Maple computations of the author which verify the sufficient condition of [7, Theorem 3.1]). EP holds for rings of the form $\mathbb{Z}/(2^\beta)$, $\mathbb{Z}/(3^\beta)$, and for finite fields $\mathbb{F}_p$ with $p = 2q + 1$, q prime (work in preparation). We conjecture that EP holds for all N.*

Example 3.6 *Euclidean weight on $R = \mathbb{Z}/(N)$. Set $a_r = |r|^2$, where representatives lie in the range $-N/2 < r \leq N/2$. Same as for Lee weight, $\mathrm{Sym}(w) = \{\pm 1\}$. EP has the same status and conjecture as for Lee weight.*

4 A Uniqueness Theorem

Theorem 4.1 *Assume R, w satisfy EP and that $a_r \in \mathbb{Q}$ in (3.1). Fix an R-module M. Then the mapping*

$$W : \mathbb{Q}[\mathcal{O}^\sharp] \to \mathbb{Q}[\mathcal{O}],$$

defined as in Theorem 3.3, is an isomorphism of $\mathbb{Q}$-vector spaces.

Corollary 4.2 *Assume the conditions of Theorem 4.1, and fix an R-module M. Then the set of scale equivalence classes of nondegenerate virtual linear* *codes* (M, η) *of constant weight over* R *forms a one-dimensional subspace of* $\mathbb{Q}[\mathcal{O}^\sharp]$.

We now interpret Corollary 4.2 in classical terms. Given a linear code $C = (M, \eta)$, the d-fold *replication* of C is the linear code $dC = (M, d\eta)$, i.e., every multiplicity $\eta(\lambda)$ is multiplied by a factor of d. In classical coding terminology, we repeat d times each column of a generator matrix for C.

Theorem 4.3 *Assume the conditions of Theorem* 4.1*. If* M *underlies a classical linear code of constant weight, then there is a nondegenerate classical linear code* (M, η) *of constant weight which has minimal length, and it is unique up to equivalence. Any other nondegenerate classical linear code* (M, η') *of constant weight is a* d*-fold replication of* (M, η)*, up to equivalence.*

Moreover, if the multiplicity function η *of a virtual linear code* (M, η) *of constant weight attains both positive and negative values, then there is* no *classical linear code of constant weight with underlying module* M*.*

5 Existence: Basic Strategy

Because of Corollary 4.2, questions of existence boil down to "guess and check": guess what the answer should be and then check that it is correct. All the guesses are based on extensive calculations—none of which appear in this paper. All the guesses can be verified to have constant weight. The details of the verifications are omitted due to lack of space.

Underlying the verifications is a simple observation. Suppose $E \subset M^\sharp$ is a submodule of linear functionals and $x \in M$. Then $\check{x} : E \to R$, $\lambda \mapsto \lambda(x)$, is an R-linear homomorphism. Its image $\operatorname{im} \check{x} \subset R$ is an ideal, and every element of $\operatorname{im} \check{x}$ is hit $|\ker \check{x}|$ times. Thus,

$$\sum_{\lambda \in E} a_{\lambda(x)} = |\ker \check{x}| \sum_{r \in \operatorname{im} \check{x}} a_r = \frac{|E|}{|\operatorname{im} \check{x}|} \sum_{r \in \operatorname{im} \check{x}} a_r. \tag{5.1}$$

We then show that expressions built up from sums of this type are independent of the choice of nonzero x. The exact expressions for the sums $\sum_{r \in \operatorname{im}(\check{x})} a_r$ depend heavily upon the particular weight function used.

Assuming the validity of EP, Theorem 4.3 provides the classification of constant weight codes, once questions of existence have been settled. This information will not be repeated for every example.

6 Hamming Weight

Theorem 6.1 *Let $R = \mathbb{Z}/(N)$, and let M be any module over R. We assume the notation in* (2.1) *and* (2.2)*, in particular that $k_{i,\beta_i} \geq 1$. Set $K_i = \sum_{j=1}^{\beta_i} k_{i,j}$. For every nonzero $\lambda \in M^\sharp$, assign the multiplicity*

$$\eta(\lambda) = \prod_{\substack{i: \\ \lambda \in p_i M^\sharp}} \left(1 - p_i^{K_i - 1}\right).$$

The resulting virtual linear code has constant Hamming weight

$$|M| \prod_{i=1}^{l} (1 - 1/p_i).$$

Corollary 6.2 *Over $R = \mathbb{Z}/(N)$, an R-module M as in* (2.2) *underlies a classical linear code of constant Hamming weight only in the following circumstances:*

- *$N = p$, a prime, with $\eta(\lambda) = 1$ for all nonzero $\lambda \in M^\sharp$, see Remark* 6.3*, or*
- *M is free of rank* 1*.*

Remark 6.3 *Let us examine carefully the case where R is the finite field $\mathbb{F}_q$. Suppose M is a k-dimensional vector space over $\mathbb{F}_q$. Since* $\mathrm{Sym}(w) = \mathbb{F}_q^\times$*, we see that every nonzero* $\mathrm{Sym}(w)$*-orbit has $q-1$ elements. Thus $\eta_S(\lambda) = q-1$ for all nonzero λ. As in Theorem* 4.3*, the shortest length code of this dimension has $\eta_S(\lambda) = 1$.*

In classical terms, the code has a generator matrix whose columns consist of one representative from each one-dimensional subspace of $\mathbb{F}_q^k$. This reproves a classical result ([2])*.*

7 Lee Weight

Write (2.1) as $N = 2^{\beta_0} p_1^{\beta_1} \cdots p_l^{\beta_l}$ (the p_i being odd primes).

Theorem 7.1 *Let $R = \mathbb{Z}/(N)$ and M be as above. To every nonzero $\lambda \in M^\sharp$, assign the multiplicity*

$$\eta(\lambda) = \prod_{\substack{1 \leq i \leq l: \\ \lambda \in p_i M^\sharp}} \left(1 - p_i^{K_i - 2}\right).$$

The resulting virtual linear code has constant Lee weight

$$(N/4)\,|M|\prod_{i=1}^{l}(1-1/p_i^2).$$

Corollary 7.2 *Over $R=\mathbb{Z}/(N)$, an R-module M underlies a classical linear code of constant Lee weight only in the following circumstances:*

- *$N=p$, a prime, M arbitrary, with $\eta(\lambda)=1$ for all nonzero $\lambda\in M^\sharp$.*
- *$N=2^{\beta_0}$, M arbitrary, $\eta(\lambda)=1$: Carlet,* [3].
- *N arbitrary, but M restricted by $K_i\le 2$, for all $i=1,2,\ldots,l$.*

8 Euclidean Weight

We still work over $R=\mathbb{Z}/(N)$, with prime factorization $N=2^{\beta_0}p_1^{\beta_1}\cdots p_l^{\beta_l}$.

For ease of exposition, we will consider several cases, starting with the case where N is odd (i.e., $\beta_0=0$).

Lemma 8.1 *Suppose N is odd. When summing over ideals of R, Euclidean weight is proportional to Lee weight by a factor of $N/3$.*

PROOF. Let $r|N$, with $ur=N$. We calculate $\sum_{s\in(r)}a_s$, for both Lee and Euclidean weights. Exploiting $\pm$-symmetry, we find that

$$\begin{aligned}\sum_{s\in(r)}a_s &= 2\sum_{t=1}^{(u-1)/2}a_{tr}\\
&=\begin{cases}2(r+2r+\cdots+r(u-1)/2) & \text{Lee}\\ 2(r^2+(2r)^2+\cdots+(r(u-1)/2)^2) & \text{Euclidean}\end{cases}\\
&=\begin{cases}r(u^2-1)/4 & \text{Lee}\\ (N/3)\cdot r(u^2-1)/4 & \text{Euclidean.}\end{cases}\qquad\square\end{aligned}$$

Theorem 8.2 *A virtual linear code over $\mathbb{Z}/(N)$, N odd, has constant Euclidean weight if and only if it has constant Lee weight. For N odd, constant Euclidean weight codes are given by Theorem* 7.1 *and Corollary* 7.2*. The weights are multiplied by a factor of $N/3$.*

We now turn to the cases where N is even ($\beta_0 > 0$). The answers depend on whether N is a power of 2 or not. In either case, we filter the module $M^\sharp$:

$$M^\sharp \supset 2M^\sharp \supset \cdots \supset 2^{\beta_0 - 1} M^\sharp \supset 2^{\beta_0} M^\sharp. \tag{8.1}$$

For nonzero $\lambda \in M^\sharp$, define $\nu(\lambda)$ to be the largest integer $\leq \beta_0$ such that $\lambda \in 2^{\nu(\lambda)} M^\sharp$.

We define some new quantities in terms of the numbers $k_{0,j}$ of (2.3). Set $e_0 = 1$ and, for $1 \leq i \leq \beta_0$, set

$$e_i = k_{0,1} + 2k_{0,2} + \cdots + (i-1)k_{0,i-1} + i(k_{0,i} + \cdots + k_{0,\beta_0}) - i. \tag{8.2}$$

Let us now turn to the case where $N = 2^{\beta_0}$ is a power of 2. In this situation, $2^{\beta_0} M^\sharp = 0$ in (8.1), so that $\nu(\lambda) \leq \beta_0 - 1$, for all nonzero $\lambda \in M^\sharp$.

Theorem 8.3 ([6]) *Let $R = \mathbb{Z}/(N)$, $N = 2^{\beta_0}$; let M be a module over R, as above. For every nonzero $\lambda \in M^\sharp$, assign the multiplicity*

$$\eta(\lambda) = \sum_{i=0}^{\nu(\lambda)} 2^{e_i}.$$

The resulting linear code is classical, has constant Euclidean weight $2^{2\beta_0 - 2} |M| = (N^2/4)|M|$, and has length

$$n = \frac{|M|}{2^{\beta_0 - 1}} \left(3 \cdot 2^{\beta_0 - 1} - 1\right) - \sum_{i=0}^{\beta_0 - 1} 2^{e_i}.$$

Finally, we consider the general even case where $N = 2^{\beta_0} p_1^{\beta_1} \cdots p_l^{\beta_l}$, $\beta_0 > 0$, $l \geq 1$. As above, set $K_i = \sum_{j=1}^{\beta_i} k_{i,j}$. Using (8.2), define

$$e'_0 = e_0, \ldots, e'_{\beta_0 - 1} = e_{\beta_0 - 1}, e'_{\beta_0} = e_{\beta_0} + 1.$$

Theorem 8.4 *Suppose $R = \mathbb{Z}/(N)$, $N = 2^{\beta_0} p_1^{\beta_1} \cdots p_l^{\beta_l}$, $\beta_0 > 0$, $l \geq 1$, M as above. For every nonzero $\lambda \in M^\sharp$, assign the multiplicity*

$$\eta(\lambda) = \left(\sum_{i=0}^{\nu(\lambda)} 2^{e'_i} \right) \prod_{\substack{1 \leq i \leq l: \\ \lambda \in p_i M^\sharp}} \left(1 - p_i^{K_i - 2}\right).$$

The resulting virtual linear code has constant Euclidean weight

$$(N^2/4)|M| \prod_{i=1}^{l} (1 - 1/p_i^2).$$

Corollary 8.5 *Over $R = \mathbb{Z}/(N)$, an R-module M underlies a classical linear code of constant Euclidean weight only in the following circumstances:*

- *$N = p$, a prime, M arbitrary, with $\eta(\lambda) = 1$ for all nonzero $\lambda \in M^\sharp$.*
- *$N = 2^{\beta_0}$, M arbitrary: Theorem 8.3.*
- *N arbitrary, but M restricted by $K_i \leq 2$, for all $i = 1, 2, \ldots, l$.*

Acknowledgements

The author thanks Purdue University Calumet, the University of Notre Dame, and Western Michigan University for sabbatical support. I thank J. Wolfmann, Ph. Langevin, and the research group GRIM at Université Toulon-Var for their hospitality during the spring of 2000. I also thank H. N. Ward for some key ideas and E. S. Moore for many things.

References

[1] E. F. Assmus, Jr. and H. F. Mattson, Error-correcting codes: An axiomatic approach, *Inform. and Control* **6** (1963) 315–330.

[2] A. Bonisoli, Every equidistant linear code is a sequence of dual Hamming codes, *Ars Combinatoria* **18** (1984) 181–186.

[3] C. Carlet, One-weight $\mathbb{Z}_4$-linear codes, in: J. Buchmann, T. Høholdt, H. Stichtenoth, and H. Tapia-Recillas, eds., *Coding Theory, Cryptography and Related Areas* (Springer, Berlin, 2000) 57–72.

[4] F. J. MacWilliams, Error-correcting codes for multiple-level transmission, *Bell System Tech. J.* **40** (1961) 281–308.

[5] J. A. Wood, Duality for modules over finite rings and applications to coding theory, *Amer. J. Math.* **121** (1999) 555–575.

[6] J. A. Wood, Linear codes over $\mathbb{Z}/(2^k)$ of constant Euclidean weight, in: *Proceedings of the Thirty-Seventh Annual Allerton Conference on Communication, Control, and Computing* (University of Illinois, 1999) 895–896.

[7] J. A. Wood, Weight functions and the extension theorem for linear codes over finite rings, in: R. C. Mullin and G. L. Mullen, eds., *Finite fields: Theory, Applications and Algorithms* (Amer. Math. Soc., Providence, 1999) 231–243.